AO 106 (Rev. 04/10) Application for a Search Warrant

UNITED STATES DISTRICT COURT

for the

Western District of Washington

In the Matter of the Search of
(Briefly describe the property to be searched or identify the person by name and address)

The Electronic Communications and Information Contained in Two (2) Cellular Devices, More Fully Described in Attachment A

Case No. MJ15-184

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A, attached hereto and incorporated herein by reference.

located in the Western District of Washington, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B, attached hereto and incorporated herein by reference.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☑ evidence of a crime;
- ☑ contraband, fruits of crime, or other items illegally possessed;
- ☑ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	*Offense Description*
18 U.S.C. 1344	Bank Fraud
18 U.S.C. 1028A(a)(1)	Aggravated Identity Theft

The application is based on these facts:
See Affidavit of Michael Spiess, attached hereto and incorporated herein.

- ☑ Continued on the attached sheet.
- ☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Special Agent Michael Spiess, U.S. Secret Service
Printed name and title

Sworn to before me and signed in my presence.

Date: April 28, 2015

Judge's signature

City and state: Seattle, Washington

MARY ALICE THEILER, U.S. MAGISTRATE JUDGE
Printed name and title

USAO# 2014R01072

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched comprises the following two cellular telephones currently in the possession of the United States Secret Service:

- TT-1: Black Samsung cell phone, model number: SM-G386T, serial number: R28F80Z85RP;
- TT-2: Black ZTE cell phone, model number: Z970, international mobile equipment identity (IMEI) number: 865891022064923.

ATTACHMENT B

ITEMS TO BE SEIZED

The following items, records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. §§ 1344 (Bank Fraud) and 1028A(a)(1) (Aggravated Identity Theft):

1. Assigned telephone numbers and identifying serial numbers (e.g., ESN, MIN, IMSI, IMEI);
2. Stored lists of received, sent, or missed calls;
3. Stored contact information;
4. Stored photographs of currency, checks, other bank account records, bank transactions, banking centers, and/or the user of the phone or suspected co-schemers, including any embedded GPS data associated with those photographs;
5. Evidence of passwords, personal identification numbers, and other features designed to encrypt or otherwise protect the content of the devices;
6. Notes taken inside applications of the various devices constituting evidence of the offenses;
7. Stored messages, including text messages of any type (SMS, MMS), instant messages, as well as email messages; and
8. Bank account records, personal identifying information, checks, deposit slips, passwords, PIN numbers, and other information related to accessing bank accounts and conducting account transactions; and
9. GPS or other geo-location data contained in the devices' memory and/or inside any navigation applications.

The search warrant authorizes imaging or otherwise copying all data contained on the subject devices. The search warrant also authorizes reasonable efforts to overcome any passcode protection of the subject devices.

AFFIDAVIT OF MICHAEL A. SPIESS

STATE OF WASHINGTON)
) ss
COUNTY OF KING)

I, MICHAEL A. SPIESS, being first duly sworn on oath, depose and say:

AGENT BACKGROUND

1. I am a Special Agent with the United States Secret Service ("USSS") and have been since September 22, 2002. I am currently assigned to the Seattle Field Office. I am a graduate of the Federal Law Enforcement Training Center located in Glynco, Georgia, and the USSS Special Agent Training Program located in Beltsville, Maryland. Before becoming a Special Agent, I was employed with the USSS as a Uniformed Officer in Washington, D.C. Before that, I served as a United States Immigration Inspector in Toronto, Canada. I have a Bachelor of Arts Degree from Daemen College in Amherst, New York. In the course of my official duties as a Special Agent, I have investigated a broad range of financial crimes, including credit card fraud, bank fraud, access device fraud, money laundering, and counterfeit currency and securities. As a result, I have experience with various methods an practices used by criminals to defraud banks and other financial institutions, including through various types of account takeover schemes.

PURPOSE OF THIS AFFIDAVIT

2. I make this affidavit in support of an application for a search warrant to search the cellular telephones more particularly described in Attachment A, which is incorporated herein by reference, for the items described in Attachment B, which is also incorporated herein by reference, all of which constitute evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1344 (Bank Fraud) and 1028A(a)(1) (Aggravated Identity Theft):

- TT-1: Black Samsung cell phone, model number: SM-G386T, serial number: R28F80Z85RP seized from RELONNA DOLLINN WARD;
- TT-2: Black ZTE cell phone, model number: Z970, international mobile equipment identity (IMEI) number: 865891022064923 seized from JOHNATHAN TURNER;

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

3. TT-1 and TT-2 were seized from RELONNA DOLLINN WARD and JOHNATHAN MARQUIEL TURNER incident to their arrest by federal agents on February 26, 2015. On February 25, 2015, a Grand Jury sitting in the Western District of Washington returned an indictment against WARD, TURNER, and eight other defendants, charging each with three counts of Bank Fraud and three counts of Aggravated Identity Theft.

4. The information contained in this affidavit is based upon my personal knowledge, my training and experience, and information collected during this investigation through, among other things, witness/suspect interviews, law enforcement investigative reports, bank statements and account records, video surveillance footage, and public records. Because this affidavit is submitted for the limited purpose of establishing probable cause, I have not set forth each and every fact known to me at present. Instead, I have included only those facts I believe necessary to establish probable cause.

5. I believe there is probable cause to conclude that WARD and TURNER (along with a number of others) participated in an account takeover scheme known as a "Bank Liq." In a Bank Liq, suspects use legitimate bank accounts to deposit counterfeit or unauthorized (and often stolen) checks. They then make cash withdrawals and/or debit card purchases, drawing down the account balance. The scheme is effective because banks often make some portion of the deposited funds available to the account holder even though it may take a few days for the invalid nature of the check to be detected and the deposit reversed. It is also common for suspects to repeat this process several times before the victim financial institution detects the fraudulent pattern and suspends/closes the account.

6. In order to conceal their activities, Bank Liq perpetrators generally avoid using their own bank accounts. Instead, they use bank accounts in others' names by either stealing account information or, often as not, with the assistance of the true account holder. The accounts involved in the instant scheme largely fall into the latter category. It appears many of these account holders were to some degree complicit in the scheme, notwithstanding their statements to the contrary. That said, there are a few instances in which the true account holders appear to have been duped into sharing their account information.

7. The account activity associated with a Bank Liq has a distinct pattern. Before it begins, the account balance is often minimal or even slightly negative. Then begins a series of deposits and

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

subsequent cash advances/debit card purchases followed by a corresponding series of deposit reversals as the deposited checks are returned once their fraudulent nature becomes apparent.

8. This investigation began in June 2013 when Bank of America security personnel notified the Seattle Field Office of the USSS of a suspected Bank Liq scheme operating in and around Seattle. Although Bank of America first reported the fraudulent activity, other financial institutions with a presence in Seattle have reported Bank Liq activity involving their accounts and the same suspects involved with the Bank of America accounts. All of these institutions are federally insured.

9. Between 2010 and 2014, the co-schemers used more than 200 bank accounts to execute this Bank Liq, carrying away nearly $1 million in ill-gotten gains. I have identified WARD and TURNER as two of dozens of participants in the scheme. Thus far, I have identified at least 73 Bank of America accounts that WARD and TURNER (working with others) used to perpetrate this Bank Liq scheme and traced at least $282,936.00 in losses to WARD's and TURNER's fraudulent activity. Each of these compromised accounts displays the hallmarks of a Bank Liq: that is, multiple check deposits, each followed by cash withdrawals/debit card purchases, only to have the checks returned days later as either unauthorized or fictitious and the victim institution unable to recover the funds withdrawn.

Fraudulent Account Activity

10. In the paragraphs that follow, I detail a portion of the fraudulent activity conducted by TURNER and WARD as part of the scheme. But the transactions described below constitute only a fraction of the total volume of fraudulent account activity in which WARD and TURNER engaged.

M.S.'s Bank of America Checking Account '6927

11. As part of this investigation, I obtained records from Bank of America related to Bank of America checking account '6927, including records of account activity and surveillance footage taken at area banking centers documenting certain account activity. Those records show that M.S. opened this account on March 20, 2014.

12. Account records also show the following: On March 21, 2014, someone made a $2,154.30 check deposit into M.S.'s Bank of America checking account '6927 and received $1,000.00 as cash back at the 72nd & Pacific Banking Center in Tacoma. On March 21, 2014, someone made a $2,324.80 check deposit into M.S.'s Bank of America checking account '6927 and received $1,000.00

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

as cash back at the Hawks Prairie Safeway Banking Center in Lacey. On March 24, 2014, someone made a $2,366.40 check deposit into M.S.'s Bank of America checking account '6927 and received $1,000.00 as cash back at the Fairwood Banking Center in Renton. Several days later, however, the deposited checks were returned due to a stop payment order and the deposits reversed.

13. As part of this investigation, I obtained Washington DOL records for WARD, including her Washington DOL photo. I compared that photo to the surveillance footage documenting the three deposits described above. Based on this comparison, I determined that WARD is the person shown in the surveillance footage. I also reviewed records documenting the deposit transactions, which show that in order to make these deposits, WARD used M.S.'s debit card with the number ending '1989 and associated PIN.

14. Account records also show that following each of these deposits but before the checks were returned to Bank of America, a portion of the deposited funds were withdrawn through either cash withdrawals or merchandise purchases at an area retailer.

15. On April 10, 2014, M.S. filed a fraud claim with Bank of America stating that the activity on M.S.'s account was unauthorized. In my experience, it is not uncommon for account holders who have provided their information to the perpetrators of a Bank Liq (often at their direction) to file fraud claims, both to avoid suspicion and in hopes of recovering additional funds from the financial institution.

16. Bank of America suspended the account and ultimately closed it due to the suspected fraud. Bank of America suffered a total loss of $11,565.83 as a result of the Bank Liq activity on this account.

17. In total, I identified video surveillance depicting WARD conducting Bank Liq activity in more than 50 bank accounts between March 2013 and January 2015. The losses on these accounts exceed $200,000.00.

A.L.'s Bank of America Checking Account '3713

18. As part of this investigation, I obtained records from Bank of America related to Bank of America checking account '3713, including records of account activity and surveillance footage taken at

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

area banking centers documenting certain account activity. Those records show that A.L. opened this account on August 19, 2014.

19. Account records also show the following: On September 11, 2014, someone made a $2,581.78 check deposit into A.L.'s Bank of America checking account '3713 and received $900.00 as cash back at the Ballard Banking Center in Seattle. On September 11, 2014, someone made a $2,386.08 check deposit into A.L.'s Bank of America checking account '3713 and received $900.00 as cash back at the University Village Banking Center in Seattle. Several days later, however, the checks were returned due to a stop payment order and the deposits reversed.

20. As part of this investigation, I obtained Washington DOL records for TURNER, including his Washington DOL photo. I compared that photo to the surveillance footage documenting the two deposits described above. Based on this comparison, I determined that TURNER is the person shown in the surveillance footage. I also reviewed records documenting the deposit transactions, which show that in order to make these deposits, TURNER used A.L.'s debit card with the number ending '9898 and associated PIN.

21. Account records also show that following each of these deposits but before the checks were returned to Bank of America, a portion of the deposited funds was withdrawn through either cash withdrawals or merchandise purchases at area retailers.

22. On September 12, 2014, A.L. filed a fraud claim with Bank of America, stating that A.L.'s Bank of America bank card and PIN were lost and the activity on his account was unauthorized. As noted above, in my experience, it is not uncommon for account holders who have provided their information to the perpetrators of a Bank Liq (often at their direction) to file fraud claims, both to avoid suspicion and in hopes of recovering additional funds from the financial institution.

23. Bank of America suspended the account and ultimately closed it due to the suspected fraud. Bank of America suffered a total loss of $4,942.44 as a result of the Bank Liq activity on this account.

24. In total, I identified video surveillance depicting TURNER conducting Bank Liq activity in 14 different Bank of America accounts between February 2013 and September 2014. The losses on these accounts totaled more than $60,000.00.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

Use of Cellular Telephones

25. I know from my training and experience that cellular telephones are an important tool for those engaged in a Bank Liq. Cellular telephones provide easy storage for and quick access to account information, personal identifiers, contacts, and other information that a Bank Liq perpetrator needs ready at hand. Because it is common for perpetrators to run a Bank Liq on multiple accounts simultaneously, the task of organizing this information is complex. Cellular telephones provide a digital storage medium that avoids the need to maintain extensive paper records. Having this information available electronically also allows perpetrators to access it more quickly and less obtrusively, reducing the likelihood that they will draw the suspicion of a merchant or bank teller while conducting a transaction.

26. Cellular telephones likewise serve an important logistical role, facilitating easy communication among co-schemers. After all, the logistics of a Bank Liq are often complex. Long-term success requires access to a constant stream of forged/stolen checks, bank accounts/associated personal identifiers, and manpower. Generally, these schemes are orchestrated by a small number of managers who recruit others to assist with the tasks of procuring checks and account information and conducting the necessary account transactions. Success depends on easy, reliable flow of checks, account information, and proceeds. Cellular telephones thus provide a critical link between the various members of the scheme.

27. The scheme at issue here is no different. As noted above, the investigation to date has revealed a massive, long-running fraud involving dozens of participants and hundreds of different bank accounts. Account records and video surveillance demonstrate a consistent flow of checks, account information, and (presumably) proceeds between and among the co-schemers. In addition to using stolen and unauthorized checks, co-schemers deposited numerous forged checks drawn on legitimate business accounts but made payable to the various account holders. For example, forged checks drawn on valid business accounts belonging to such companies as Amazon, the University of Washington, Boeing, Target, and Trader Joe's were deposited into multiple accounts during the course of these scheme. Account information also passed through multiple hands. The video surveillance obtained during this investigation shows that in many cases multiple suspects conducted Bank Liq activity within

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

the same account. It is difficult to imagine how this scheme could have continued and succeeded as it did without the aid of cellular telephones.

28. In the course of this investigation, I also identified many instances in which co-schemers used cellular telephones to access Bank of America's automated account access system. From this system, account holders (or those with the account holders' personal information) can perform a number of tasks that can be of use to a Bank Liq perpetrator. For example, the system allows balance inquiries, permitting the caller to confirm whether funds from a given deposit have been made available for withdrawal. Just as important, the system allows an account holder to increase withdrawal limits limits, thereby increasing the daily limits on cash withdrawals and increasing the fraudster's revenue from the scheme.

29. As part of this investigation, another officer and I conducted several interviews of R.B., a member of the Bank Liq scheme. R.B. was initially arrested in Lewis County and charged with state-law crimes related to her Bank Liq activity. R.B. agreed to cooperate with law enforcement in hopes of receiving more lenient treatment. It should be noted, however, that R.B. was not entirely truthful in her discussions with law enforcement. She attempted to conceal, among other things, the extent of her participation in the scheme and her knowledge about the identities of other participants. R.B. did identify WARD as one of the individuals who oversaw her participation in the scheme, including by providing transportation to bank branches and directing R.B. in executing the scheme. Among other things, R.B. explained that during her trips with WARD, WARD would use both her own and R.B.'s cellular telephone to access Bank of America's automated account information system and increase the withdrawal limit for the account the two were using to accomplish the Bank Liq.

30. During this investigation, I have identified several cellular telephone numbers linked to WARD. These include the number 206-434-9119. A February 10, 2015, search of a law enforcement database shows WARD as the subscriber for this number. A Tacoma Police Department report (Incident #141950706) dated July 14, 2014, lists WARD's phone number as 253-227-0818. And a Puyallup Police Department report (Incident # 14000874) dated February 1, 2014, lists WARD phone number as 253-267-2400.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

31. Bank of America records show that each of these telephone numbers has been used to access bank accounts involved in Bank Liq scheme. Indeed, forty different bank accounts were accessed by one of these three telephone numbers during the execution of the scheme. There is video surveillance documenting fraudulent activity WARD involving all but four of these accounts, most recently in January 2015.

MANNER OF SEARCH

32. I intend to deliver TT-1 and TT-2 to a forensic examiner who will recover data from TT-1 and TT-2 using computer forensic best practices.

33. Law enforcement will ensure that only data physically located on TT-1 and TT-2 will be recovered, in that the phones will be disabled from accessing a mobile phone network or wifi access point. This process will not capture data stored on any other server, such as emails that have not been previously downloaded to the phones.

34. The examiner will apply a software program that will extract from TT-1 and TT-2 the information identified in Attachment B. The examiner will provide me either only these data or data in a form in which these areas will be clearly delineated. I intend to search each of the phones for the items that are described in Attachment B.

35. If the forensic examiner is unable to use a software program to extract data from any of the phones, I intend to instead manually search the phones by looking at the applicable sections of the actual phones for the items that are described in Attachment B.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

CONCLUSION

36. In sum, I believe there is probable cause to believe that the Target Telephones contain evidence, fruits, and instrumentalities of violations of Title 18, United States Code, Sections 1344 and 1028A(a)(1). I seek authorization to search the Target Telephones for the items that are described in Attachment B.

MICHAEL A. SPIESS
Special Agent, U.S. SECRET SERVICE

SUBSCRIBED AND SWORN before me this 28 day of April, 2015.

MARY ALICE THEILER
U.S. MAGISTRATE JUDGE

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT A

PROPERTY TO BE SEARCHED

The property to be searched comprises the following two cellular telephones currently in the possession of the United States Secret Service:

- TT-1: Black Samsung cell phone, model number: SM-G386T, serial number: R28F80Z85RP;
- TT-2: Black ZTE cell phone, model number: Z970, international mobile equipment identity (IMEI) number: 865891022064923.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970

ATTACHMENT B

ITEMS TO BE SEIZED

The following items, records, documents, files, or materials, in whatever form, that constitute evidence, instrumentalities, or fruits of violations 18 U.S.C. §§ 1344 (Bank Fraud) and 1028A(a)(1) (Aggravated Identity Theft):

1. Assigned telephone numbers and identifying serial numbers (e.g., ESN, MIN, IMSI, IMEI);
2. Stored lists of received, sent, or missed calls;
3. Stored contact information;
4. Stored photographs of currency, checks, other bank account records, bank transactions, banking centers, and/or the user of the phone or suspected co-schemers, including any embedded GPS data associated with those photographs;
5. Evidence of passwords, personal identification numbers, and other features designed to encrypt or otherwise protect the content of the devices;
6. Notes taken inside applications of the various devices constituting evidence of the offenses;
7. Stored messages, including text messages of any type (SMS, MMS), instant messages, as well as email messages; and
8. Bank account records, personal identifying information, checks, deposit slips, passwords, PIN numbers, and other information related to accessing bank accounts and conducting account transactions; and
9. GPS or other geo-location data contained in the devices' memory and/or inside any navigation applications.

The search warrant authorizes imaging or otherwise copying all data contained on the subject devices. The search warrant also authorizes reasonable efforts to overcome any passcode protection of the subject devices.

UNITED STATES ATTORNEY
700 STEWART STREET, SUITE 5220
SEATTLE, WASHINGTON 98101
(206) 553-7970